



Ira-governmental Payment and Collection System

Master Administrator Designation Form

Check one box:

- ☐ New Request
☐ Revoke

Master Administrator

Name (First, Middle Initial, Last) _____
Agency/Department Name _____
Bureau _____
Street Address 1 _____
Street Address 2 _____
City, State Zip code _____
Country _____ E-mail Address _____
Telephone Number _____

Please check **one** of the following: Is this Master designated at Agency/Department Level ☐
Bureau Level ☐

Complete the appropriate table(s) below, providing the Agency Location Codes (ALCs) of the Master Administrator.

ALC	ALC	ALC	ALC

Name of CFO or Deputy CFO

Signature of CFO or Deputy CFO

Telephone #

Date

For FMS Administrator USE ONLY: (Complete this section when you have completed a review of the request)

_____ FMS Administrator Name	_____ FMS Administrator Signature	_____ Telephone #	_____ Date
---------------------------------	--------------------------------------	----------------------	---------------



Due Diligence Guidelines

It is very important to verify the identity of the Federal Program Agency¹, their Master Administrator², Agency Administrator³, and End User⁴. The general rule is the more sensitive the information, the more exhaustive the verification process.

1. The Federal Program Agency will provide a name of a Master Administrator² per Agency/Department or Bureau designated with the authority to determine whether an Agency Administrator (AA) should be authorized as an Agency Administrator for the IPAC application(s).
2. The Master Administrator will designate at least two support contacts as Agency Administrators. One contact name shall be designated as Primary and the other(s) as Alternate(s). The individuals identified as Agency Administrators must have the level of authority at the Federal Program Agency to determine whether an End User should be given access to the requested IPAC application(s).

Note: A Master Administrator cannot be a User or an Agency Administrator

3. After the Master Administrator has received a signed Agency Administrator Responsibility Agreement and signed Rules of Behavior from the Agency Administrator(s), they can approve the AAs access in the Treasury Web Application Infrastructure (TWAI) User Provisioning Service (UPS), initially FMS will accept completed AA Designation Forms from the MA, and issue the AA(s) their IPAC application(s) and functional roles.
4. Once the AA has received a signed user request form and signed Rules of Behavior from the user, the AA can approve access to the IPAC Application in the TWAI; FMS will accept completed forms from the AA and issue the End User IPAC application(s) and functional roles.
5. Registration Forms containing the name and other required identification of the individual End User requesting a Logon ID and application access will be completed by either the End User or the Agency Administrator, or Master Administrator. The responsible Administrator must verify the End User and can be authorized to access the application(s), which have been requested. At a minimum, this will require the signature of the End User's management on the Registration Form. Other existing procedures may also be used.

Note: If the Agency Administrator is also the End User's management, the alternate Agency Administrator should verify the request.

6. After the End User is verified and the request is authenticated, the Administrator can then process the request.

¹ **Federal Program Agency** – business entity requiring access to the IPAC system.

² **Master Administrator** - term for the individual(s) identified formally by the CFO or Deputy CFO as trusted to authorize requests for other individual(s) at their Agency to access the IPAC system on their behalf.

³ **Agency Administrator** – term for the individual(s) identified formally by the Master Administrator as trusted to authorize requests for other individual(s) at their Agency to access the IPAC system on their behalf.

⁴ **End User** – an individual person employed by a Federal Program Agency who has a business need for access to the IPAC system.

Fax completed form, along with the signed Rules of Behavior and signed Responsibility Agreement, to the Treasury Support Center at 314-444-7346



Agency Administrator Responsibility Agreement

This form is in compliance with the Privacy Act of 1974 (Section 552a, 5 U.S.C.), Section 301, 5 U.S.C., Section 3105, 44 U.S.C., 18 U.S.C. 3056, and the Treasury Departmental Offices Directive DO 216. The information you provide on this form will be used principally to aid in the completion of your access request to FMS systems. All or part of this information may be furnished to Federal, State, local and public agencies in the event a violation of law is disclosed.

Completion of this form is voluntary; however, failure to complete the form requested will result in no consideration for access to FMS systems. Although no penalties are authorized if you do not provide the requested information, failure to supply information will result in your not receiving access to FMS systems.

Responsibilities:

I am aware that the *Financial Management Service (FMS)* policy is to treat all information as an asset, whether it is computer programs, software, data or other information collected, stored, and generated in the conduct of its business. To the best of my ability, I will protect information from unauthorized use, modification, destruction, or disclosure, whether accidental or intentional.

I am aware of the policies and requirements of FMS and agree to abide by them.

I will NOT attempt to circumvent any of the security mechanisms within the User Provisioning Service (UPS) and IPAC system.

I will safeguard Logon IDs and Passwords entrusted in my control.

I will ensure that proper authorizations on request forms are checked.

I will ensure that all fields on the request forms are complete and correct.

I will issue Logon IDs, Passwords and Access on a need-to-know basis.

I will ensure proper record keeping of all information processed.

I will comply with all security-related policies, standards, procedures and practices.

I will notify the Treasury Support Center at 866-809-5218 of any known or suspected violation of information security policy, procedures, or threat to IPAC resources.

Master Administrator ACKNOWLEDGMENT

I have read and understand the Master Administrator Responsibility Agreement and agree to abide by it.

Print Name: _____ Date: _____

Signature: _____

Agency/Department: _____



Rules of Behavior

Terms of Use

Please read and accept the Terms of Use in order to complete your access request.

GENERAL

- **Exercise only those IPAC System capabilities assigned to you by your Organization or Unit IPAC Security Administrator.**

Each User registered to access the IPAC system will have a unique User ID. One of those specific roles may be assigned to each user. The level of authority available to a user in a role will determine the level of user authentication required to allow execution of the role. Both User ID and authentication information are the property of the IPAC System and the user. Transfer of User ID and authentication to another can result in loss of IPAC System access privileges. Attempting to exercise roles other than those assigned by any means can result in loss of IPAC System access. Only one Master Administrator will give each Agency Administrator access authority. Only one Agency Administrator will give each IPAC user access authority. Each Agency Administrator will have a backup.

- **Provide appropriate controls over sensitive information available from IPAC.**

Information available from the IPAC System may be considered sensitive (Privacy Act), sensitive (Business), restricted or classified.

Sensitive (Privacy Act) information is any information in IPAC that relates to an individual by name, social security number or traceable characteristic (User ID, telephone number, etc.) to a financial transaction affecting that individual. Sensitive (Privacy Act) information must be controlled as defined in The Privacy Act of 1974, 5 USC & 552A – as amended.

Sensitive (Business) information is any information in IPAC except that information appearing specifically on financial reports released to the Public by appropriate authority and then only in the context of the public report. Sensitive (Business) information can be released only to those individuals having a business need to see or use it.

The IPAC System will allow only those users with appropriate formal clearance to access the restricted information. If restricted information is available to you and you have neither appropriate clearance and need to know, it is your responsibility to report the incident and associated circumstance to your Agency Administrator or your Master Administrator.

- **Understand and comply with applicable policies and procedures related to your access to, and use of, IPAC resources.**

Your organization has its own policies and procedures related to access and use of information available through your organization Intranet or Internet. Your organization may have policies and procedures related to distribution of financial information within the organization and to external organizations. Your internal policies and procedures will be available through your Master Administrator or your Agency Administrator.

Fax completed form, along with the signed Rules of Behavior and signed Responsibility Agreement, to the Treasury Support Center at 314-444-7346

- **Identify potential risks to IPAC System and information integrity, timeliness or sensitivity to the appropriate organization authority.**

Since the financial management data and information in the IPAC System is the U.S. Department of the Treasury's picture related to user agency financial status, it is critical that all who use the system and data participate in identifying conditions or actions which will impede the integrity, timeliness or sensitivity of the IPAC System or data. Risks internal to your organization must be reported through your internal security point of contact. Apparent risks to the IPAC System itself must be identified through your Master Administrator, Agency Administrator, or the FMS Administrator.

- **Identify inhibitors to effective performance of your IPAC System related responsibilities to the appropriate organization authority**

Inhibitors to your effective performance of the IPAC System related tasks pertaining to intra-governmental transfers have direct impact on the integrity of IPAC information available for decision making and reporting. Inhibitors fit into two categories – IPAC System oriented and organization infrastructure or system oriented. IPAC System inhibitors to your performance include such things as time to download information, download media, content of records or screens, availability of detail to support research, and the like. To report your IPAC System inhibitors contact the Treasury Support Center at 866-809-5218.

SPECIFIC

USERS must ensure that the information technology (IT) resources with which they have been entrusted are used properly, as directed by FMS policies and standards, taking care that the laws, regulations, and policies governing the use of such resources are followed and that the value of all information assets are preserved. Each user is responsible for all activities associated with their assigned User ID.

USERS must be knowledgeable about FMS IT policies and standards. As systems change, users are required to seek additional information in order to ensure current policies and procedures are followed.

USERS must take positive steps to protect FMS data from unauthorized users.

USERS must not attempt to circumvent any FMS IT security control mechanisms.

USERS must follow proper login/logoff procedures.

USERS must complete IR security awareness, training and education as required by their agency's policies and procedures.

USERS must not read, alter, insert, copy, or delete any FMS data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular:

USERS must not browse or search FMS data except in the performance of authorized duties.

USERS must not reveal information produced by the FMS application except as required by job function and within established procedures.

USERS must protect FMS communications/connectivity integrity.

Fax completed form, along with the signed Rules of Behavior and signed Responsibility Agreement, to the Treasury Support Center at 314-444-7346

USERS must comply with and provide assistance with IT audits and reviews as appropriate

USERS must report any known or suspected breaches of IT security to security administrators immediately after discovery of the occurrence.

USERS must retrieve all hard copy printouts in a timely manner.

USERS must ensure that unauthorized individuals cannot view screen contents.

USERS must protect User IDs and passwords from improper disclosure. Passwords provide access to FMS data and resources.

USERS are responsible for any access made under his/her User ID and password.

USERS do not reveal Passwords under any circumstances. Password disclosure is considered a security violation and is to be reported as such. If Password disclosure is necessary for problem resolution, immediately select a new password once the problem has been resolved.

Do not program login IDs or Passwords into automatic script routines or programs.

Do not share Passwords with anyone else or use another person's Password.

Do not write Passwords down.

Change Passwords in accordance with the system/application requirements.

Choose hard to guess Passwords, in accordance with the system/application requirements.

ACCEPTANCE

I have read the Financial Management (FMS) Information technology Terms of Use and fully understand the security requirements of the information systems, modules and data. I further understand that violation of these rules may be grounds for administrative and/or disciplinary action by agency officials and may result in actions up to and including termination or prosecution under Federal law.

☐ **Accept** ☐ **Do Not Accept**

Print Name: _____ Date: _____

Signature: _____

Fax completed form, along with the signed Rules of Behavior and signed Responsibility Agreement, to the Treasury Support Center at 314-444-7346